(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－196982
（P2002－196982A）
(43)公開日　平成14年７月12日(2002.7.12)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
G06F 12/14	320	G06F 12/14	320B	5B017
G11B 20/10		G11B 20/10	H	5C053
H04L 9/08		H04L 9/00	601C	5D044
9/32			675A	5J104
H04N 5/91		H04N 5/91	P	

審査請求　未請求　請求項の数８　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願2000－395722(P2000－395722)

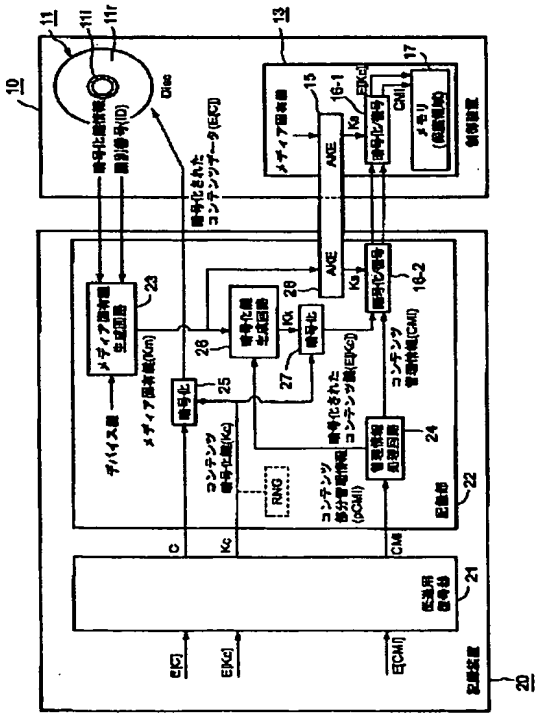
(22)出願日　平成12年12月26日(2000.12.26)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　加藤　拓
東京都府中市東芝町１番地　株式会社東芝
府中事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B017 AA01 AA06 BA07 CA09
5C053 FA13 FA25 JA21 KA01 LA15
5D044 BC04 CC04 DE17 DE50 EF05
FG18 JJ01
5J104 AA07 AA12 AA15 AA16 EA06
EA17 KA02 KA04 NA02 PA14

(54)【発明の名称】　情報記録媒体、記録／再生装置及び方法

(57)【要約】
【課題】　コンテンツデータを記録しつつ、不正な利用から保護する。
【解決手段】　著作権付コンテンツデータが再生可能に暗号化されて記録される媒体部（１１）と、著作権付コンテンツデータの記録／再生処理の可否を制御するための管理情報が記録され、且つ記録処理を行なう記録装置（２０）及び再生処理を行なう再生装置の各々に対する認証機能を有する制御装置（１３）とを備えた情報記録媒体（１０）を用いる。これにより、認証機能により認証され、且つ管理情報により記録／再生可能とされたときのみ、コンテンツデータを記録／再生できる。



【特許請求の範囲】
【請求項１】　著作権付コンテンツデータが暗号化されて記録される媒体部と、
前記著作権付コンテンツデータの記録／再生処理の可否を制御するための管理情報が記録され、且つ前記記録処理を行なう記録装置及び前記再生処理を行なう再生装置の各々に対する認証機能を有する制御装置と、
を備えたことを特徴とする情報記録媒体。
【請求項２】　請求項１に記載の情報記録媒体において、
前記制御装置は、前記媒体部から読み出された識別情報から前記記録装置又は前記再生装置が作成した記録媒体固有鍵に基づいて、前記認証機能を実行することを特徴とする情報記録媒体。
【請求項３】　請求項１又は請求項２に記載の情報記録媒体において、
前記媒体部を収容するための媒体保護手段を備えており、
前記制御装置は、前記媒体保護手段に取付けられたことを特徴とする情報記録媒体。
【請求項４】　請求項１乃至請求項３のいずれか１項に記載の情報記録媒体において、
前記媒体部と前記制御装置とは、互いに離間して設けられたことを特徴とする情報記録媒体。
【請求項５】　著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる記録装置であって、
記録対象の著作権付コンテンツデータと共に与えられる管理情報に基づいて、前記媒体部への記録処理の可否を判定する管理情報処理手段と、
前記管理情報処理手段による判定結果が記録可のとき、前記著作権付コンテンツデータを暗号化して前記媒体部に記録するコンテンツ記録手段と、
前記管理情報処理手段による判定結果が記録可のとき、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記管理情報を前記制御装置に転送する管理情報転送手段と、
を備えたことを特徴とする記録装置。
【請求項６】　著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる再生装置であって、
前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記制御装置から管理情報を読み出す管理情報読出手段と、
前記管理情報読出手段により読み出された管理情報に基づいて、前記再生処理の可否を判定する管理情報処理手段と、
前記管理情報処理手段による判定結果が再生可のとき、前記媒体部内の暗号化された著作権付コンテンツデータを復号して再生するコンテンツ復号手段と、
を備えたことを特徴とする再生装置。
【請求項７】　著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる記録方法であって、
記録対象の著作権付コンテンツデータと共に与えられる管理情報に基づいて、前記媒体部への記録処理の可否を判定する管理情報処理ステップと、
前記管理情報処理ステップによる判定結果が記録可のとき、前記著作権付コンテンツデータを暗号化して前記媒体部に記録するコンテンツ記録ステップと、
前記管理情報処理ステップによる判定結果が記録可のとき、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記管理情報を前記制御装置に転送する管理情報転送ステップと、
を含んでいることを特徴とする記録方法。
【請求項８】　著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる再生方法であって、
前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記制御装置から管理情報を読み出す管理情報読出ステップと、
前記管理情報読出ステップにより読み出された管理情報に基づいて、前記再生処理の可否を判定する管理情報処理ステップと、
前記管理情報処理ステップによる判定結果が再生可のとき、前記媒体部内の暗号化された著作権付コンテンツデータを復号して再生するコンテンツ復号ステップと、
を含んでいることを特徴とする再生方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権付コンテンツデータを記録可能で、且つ不正な利用から保護し得る情報記録媒体、記録／再生装置及び方法に関する。
【０００２】
【従来の技術】近年、著作権付コンテンツデータ等の情報を記録する分野では、ＤＶＤ等の如き、読取り専用領域及び書込可能領域といった単純な記録領域のみからなる情報記録媒体が広く知られている。
【０００３】ここで、著作権付コンテンツデータは、読取専用領域に事前に記録される場合、不正な記録装置を用いた不正な書換えから保護される。
【０００４】
【発明が解決しようとする課題】しかしながら以上のような情報記録媒体では、読取専用領域を用いるため、正当な記録装置を用いた正当な記録が実行できないことになる。一方、著作権付コンテンツデータが書込可能領域

に記録される場合、不正な記録装置を用いた不正な書換え等の利用（例、改ざん後の利用等）が可能となってしまう。

【０００５】すなわち、著作権付コンテンツデータを不正な利用から保護しつつ、正当な記録も可能な情報記録媒体が存在しない問題がある。

【０００６】本発明は上記実情を考慮してなされたもので、コンテンツデータを記録可能で、且つ不正な利用から保護し得る情報記憶媒体、記録／再生装置及び方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の骨子は、情報記録媒体のコンテンツ記録領域とは切り離された場所に制御装置を備えた構成により、単純な情報記録媒体の手軽さを維持しつつ、複雑なセキュリティ機能を実現する。

【０００８】具体的には、所定の情報記録媒体本体と、対応する制御装置との組合せのときのみ、情報記憶媒体内のコンテンツデータを利用できる構成により、レベルの高いセキュリティ機能を実現する。

【０００９】ここで、セキュリティ機能としては、例えば、コンテンツのコピー枚数制御、コンテンツのチェックイン／チェックアウト機能（http://www.Sdmi.org/, “SDMI Portable Device Specification Part 1, Version 1.0”参照）など多様なコンテンツ保護機能などがある。

【００１０】さて以上のような本発明の骨子に基づき、具体的には以下のような手段が講じられる。

【００１１】第１の発明は、著作権付コンテンツデータが暗号化されて記録される媒体部と、前記著作権付コンテンツデータの記録／再生処理の可否を制御するための管理情報が記録され、且つ前記記録処理を行なう記録装置及び前記再生処理を行なう再生装置の各々に対する認証機能を有する制御装置と、を備えた情報記録媒体である。

【００１２】これにより、認証機能により認証され、且つ管理情報により記録／再生可能とされたときのみ、コンテンツデータを記録／再生できる情報記録媒体が実現されるため、コンテンツデータを記録可能で、且つ不正な利用から保護することができる。

【００１３】第２の発明は、第１の発明において、前記制御装置としては、前記媒体部から読み出された識別情報から前記記録装置又は前記再生装置が作成した記録媒体固有鍵（以下、メディア固有鍵という）に基づいて、前記認証機能を実行する情報記録媒体である。

【００１４】これにより、媒体部と制御装置との組合せが一致しないと制御装置が相手装置（記録／再生装置）を認証しないので、第１の発明の作用に加え、制御装置又は媒体部の付替えといった改造による不正を阻止することができる。

【００１５】第３の発明は、第１又は第２の発明において、前記媒体部を収容するための媒体保護手段を備えており、前記制御装置としては、前記媒体保護手段に取付けられた情報記録媒体である。

【００１６】これにより、第１又は第２の発明が簡易な構成で実現できるので、第１又は第２の発明の作用を奏する情報記録媒体を容易且つ確実に製造することができる。

【００１７】第４の発明は、第１～第３のいずれかの発明において、前記媒体部と前記制御装置とは、互いに離間して設けられた情報記録媒体である。

【００１８】これにより、第１～第３の発明を、固定的に設けられた制御装置と、回転可能な媒体部（例、ディスク、テープ等）という構成により容易に実現できる。

【００１９】第５の発明は、著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる記録装置であって、記録対象の著作権付コンテンツデータと共に与えられる管理情報に基づいて、前記媒体部への記録処理の可否を判定する管理情報処理手段と、前記管理情報処理手段による判定結果が記録可のとき、前記著作権付コンテンツデータを暗号化して前記媒体部に記録するコンテンツ記録手段と、前記管理情報処理手段による判定結果が記録可のとき、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記管理情報を前記制御装置に転送する管理情報転送手段と、を備えた記録装置である。なお、第５の発明は、同様の技術内容をもつ記録方法として表現してもよい。

【００２０】これにより、第１の発明の作用に加え、認証機能により認証され、且つ管理情報により記録可能とされたときのみ、コンテンツデータを記録するため、コンテンツデータを不正な利用から保護することができる。

【００２１】第６の発明は、著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる再生装置であって、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記制御装置から管理情報を読み出す管理情報読出手段と、前記管理情報読出手段により読み出された管理情報に基づいて、前記再生処理の可否を判定する管理情報処理手段と、前記管理情報処理手段による判定結果が再生可のとき、前記媒体部内の暗号化された著作権付コンテンツデータを復号して再生するコンテンツ復号手段と、を備えた再生装置である。　なお、第６の発明は、同様の技術内容をもつ再生方法として表現してもよい。

【００２２】これにより、第１の発明の作用に加え、認証機能により認証され、且つ管理情報により再生可能とされたときのみ、コンテンツデータを再生するため、コンテンツデータを不正な利用から保護することができ

る。

【００２３】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照して説明する。

（第１の実施形態）図１及び図２は本発明の第１の実施形態に係る情報記録媒体の構成を示す模式図であり、図３はこの情報記録媒体及び記録装置の構成を示す模式図であり、図４はこの情報記録媒体及び再生装置の構成を示す模式図である。

【００２４】ここで、情報記録媒体１０は、図１に示すように、ＤＶＤ－ＲＡＭディスク（記録用の媒体）１１と、このＤＶＤ－ＲＡＭディスク１１を回転可能に収容する略正方形状の保護ケース１２と、この保護ケース１２の一隅に取付けられた制御装置１３とを備えている。なお、情報記録媒体１０は、保護ケース１２の内部に制御装置１３を備えた構成に限らず、保護ケース１２の外部に制御装置１３を取付けた構成としてもよい。

【００２５】ＤＶＤ－ＲＡＭディスク１１は、記録用の媒体の一例であり、ディスク内周側に位置する読出専用のリードイン（Lead-in）領域１１ｉと、このリードイン領域よりも外周側に位置する読出／書込可能な記録領域１１ｒとを備えている。なお、ＤＶＤ－ＲＡＭディスク１１は、記録用の媒体の一例であり、適宜、他種類の記録用の媒体（例、Ｄ－ＶＨＳ等）に変えてもよい。また、他種類の記録用の媒体としては、ディスク状の媒体に限らず、例えばテープ状の媒体を用いてもよい。

【００２６】リードイン領域１１ｉは、暗号化された鍵情報及び各々のＤＶＤ－ＲＡＭディスク１１を区別するための識別番号（ＩＤ）がディスク製造時に書込まれた読出専用領域である。

【００２７】記録領域１１ｒは、暗号化されたコンテンツデータＥ［Ｃ］が読出／書込可能に記録される領域である。なお、コンテンツデータＣは、ここでは著作権付きコンテンツを表現するためのデータを意味している。

【００２８】保護ケース１２は、回転可能にＤＶＤ－ＲＡＭディスク１１を保持し、そのＤＶＤ－ＲＡＭディスク１１の一部を記録時／再生時のみ露出させるためのスライド蓋付窓部１４が形成されている。

【００２９】制御装置１３は、図２に示すように、予め当該ＤＶＤ－ＲＡＭディスク１１に対応するメディア固有鍵Ｋｐを秘密に格納しており、且つ認証・鍵交換部１５、暗号化／復号回路１６－１及びメモリ１７を備えている。

【００３０】認証・鍵交換部１５は、アクセスしてきた記録装置２０又は再生装置３０の正当性を確認するため、読出／書込の際に、アクセスしてきた装置との間で自装置１３内のメディア固有鍵Ｋｐに基づいて、所定の認証及び鍵交換（ＡＫＥ：Authentication and Key Exchange）処理を行ない、共有鍵Ｋｓを記録装置２０や再生装置３０と共有するものである。

【００３１】なお、制御装置１３のメディア固有鍵Ｋｐと、記録装置２０及び再生装置３０のメディア固有鍵Ｋｍとの関係は、互いに同じ値（Ｋｐ＝Ｋｍ）としてもよく、又は、互いに違う値（Ｋｐ≠Ｋｍ、例、ＫｐとＫｍは公開鍵と秘密鍵の関係）としてもよいが、当該関係に応じて認証・鍵交換部１５の処理内容を設定する必要がある。

【００３２】暗号化／復号回路１６－１は、アクセスしてきた記録装置２０又は再生装置３０と、自装置１３との間の通信路における盗聴や改ざん等の攻撃を防ぐため、認証・鍵交換部１５により共有された共有鍵Ｋｓに基づいて、メモリ１７内のデータを暗号化して記録装置２０又は再生装置３０に送出する機能と、記録装置２０又は再生装置３０から受けた暗号化データを復号して復号結果をメモリ１７に記録する機能をもっている。

【００３３】次に、記録装置２０及び再生装置３０の構成について順次説明する。なお、記録装置２０と再生装置３０を別々に設けた場合について述べるが、これに限らず、記録装置２０と再生装置３０とを合わせた記録／再生装置として設けてもよい。また、記録装置２０及び再生装置３０は、従来同様に、自装置１３内に秘密に保持されたデバイス鍵と呼ばれる、装置固有の鍵を備えている。

【００３４】記録装置２０は、図３に示すように、伝送用復号器２１及び記録部２２を備えている。

【００３５】伝送用復号器２１は、記録装置２０内部から受ける夫々暗号化されたコンテンツデータＥ［Ｃ］、暗号化されたコンテンツ暗号化鍵Ｅ［Ｋｃ］及び暗号化されたコンテンツ管理情報Ｅ［ＣＭＩ］を復号し、夫々得られたコンテンツデータＣ、コンテンツ暗号化鍵Ｋｃ及びコンテンツ管理情報ＣＭＩ（Content ManagementInformation）を記録部２２に入力する機能をもっている。

【００３６】記録部２２は、伝送用復号器２３から得られたコンテンツデータＣ、コンテンツ暗号化鍵Ｋｃ及びコンテンツ管理情報ＣＭＩに基づいて、コンテンツ暗号化鍵Ｋｃにより暗号化して得た暗号化されたコンテンツデータＥ［Ｃ］をＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む機能と、コンテンツ暗号化鍵Ｋｃを暗号化して得た暗号化されたコンテンツ暗号化鍵Ｅ［Ｋｃ］、及びコンテンツ管理情報ＣＭＩを夫々共有鍵Ｋｓで暗号化して制御装置１３に送出する機能をもっている。なお、記録装置２０が伝送用復号器２１からコンテンツ暗号化鍵Ｋｃを入力しない方式の場合、記録部２２は、予め設けられた乱数生成器ＲＮＧにより生成した乱数をコンテンツ暗号化鍵Ｋｃとして用いても良い。

【００３７】具体的には記録部２２は、メディア固有鍵生成回路２３、管理情報処理回路２４、コンテンツ暗号化部２５、暗号化鍵生成回路２６、鍵暗号化部２７、認証・鍵交換部２８、暗号化／復号回路１６－２を備えて

いる。

【００３８】メディア固有鍵生成回路２３は、ＤＶＤ－ＲＡＭディスク１１のリードイン領域１１ｉから読み出された暗号化鍵情報及び識別情報ＩＤと、自己のデバイス鍵とに基づいてメディア固有鍵Ｋｍを生成する機能と、このメディア固有鍵Ｋｍを暗号化鍵生成回路２５及び認証・鍵交換部２８に送出する機能とをもっている。

【００３９】ここで、メディア固有鍵Ｋｍは、あるＤＶＤ－ＲＡＭディスク１１に記録されたコンテンツが正当な全ての再生装置３０で再生可能となるように、正当な全ての記録装置２０において、全て同じ値に生成される。

【００４０】管理情報処理回路２４は、伝送用復号器２１から入力されたコンテンツ管理情報ＣＭＩに基づいて記録禁止か否かを判定する機能と、判定結果が記録禁止を示すときには記録処理を終了する機能とをもっている。

【００４１】また、管理情報処理回路２４は、判定結果が否（記録可能）を示すとき、コンテンツ管理情報ＣＭＩからコンテンツ部分管理情報ｐＣＭＩを抽出する機能と、このコンテンツ部分管理情報ｐＣＭＩを暗号化鍵生成回路２６に送出すると共に、コンテンツ管理情報ＣＭＩを暗号化／復号回路１６－２に送出する機能とをもっている。

【００４２】なお、コンテンツ管理情報ＣＭＩは、コンテンツを管理するための情報であり、例えば書誌的事項を管理する内容（例、著作者や著作年月日）、コピー管理に関する内容（例、コピー可能回数）、再生管理に関する内容（例、再生可能回数）等の任意のものが適宜、設定可能である。

【００４３】コンテンツ暗号化部２５は、伝送用復号器２１からのコンテンツ暗号化鍵Ｋｃに基づいて、伝送用復号器２１から入力されたコンテンツデータＣを暗号化する機能と、得られた暗号化されたコンテンツデータＥ［Ｃ］をＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む機能とをもっている。

【００４４】暗号化鍵生成回路２６は、メディア固有鍵生成回路２３から受けたメディア固有鍵Ｋｍと、管理情報処理回路２４から受けたコンテンツ部分管理情報ｐＣＭＩとに基づいて鍵暗号化鍵Ｋｋを生成する機能と、この鍵暗号化鍵Ｋｋを鍵暗号化部に送出する機能とをもっている。

【００４５】鍵暗号化部２７は、暗号化鍵生成回路２６から受けた鍵暗号化鍵Ｋｋを用いてコンテンツ暗号化鍵Ｋｃを暗号化する機能と、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を暗号化／復号回路１６－２に送出する機能とをもっている。

【００４６】認証・鍵交換部２８は、メディア固有鍵生成回路２３から受けたメディア固有鍵Ｋｍを用いて制御装置１３の認証・鍵交換部１５との間で認証及び鍵交換（ＡＫＥ）処理を行なう機能と、鍵交換処理の結果、制御装置１３との間で共有鍵Ｋｓを共有する機能とをもっている。

【００４７】暗号化／復号回路１６－２は、認証・鍵交換部２８により共有された共有鍵Ｋｓに基づいて、鍵暗号化部２７から受けた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］と、管理情報処理回路２４から受けたコンテンツ管理情報ＣＭＩとの両者を暗号化する機能と、この暗号化により得られた暗号化データを制御装置１３に送出する機能とをもっている。なお、記録装置２０の暗号化／復号回路１６－２は、制御装置１３内の暗号化復号回路１６－１と基本的に同じ回路であり、後述する再生装置３０にも設けられている。すなわち、制御装置１３、記録装置２０及び再生装置３０の各暗号化／復号回路１６－１，１６－２同士は、基本的に同一構成であり、配置場所が異なるだけである。

【００４８】一方、再生装置３０は、図４に示すように、伝送用暗号化器３１と、再生部３２とを備えている。

【００４９】伝送用暗号化器３１は、再生部３２から受けるコンテンツデータＣ、コンテンツ暗号化鍵Ｋｃ及びコンテンツ管理情報ＣＭＩの各々を暗号化する機能と、暗号化により得られた暗号化されたコンテンツデータＥ［Ｃ］、暗号化されたコンテンツ鍵Ｅ［Ｋｃ］及び暗号化されたコンテンツ管理情報Ｅ［ＣＭＩ］を再生装置３０の内部に出力する機能とをもっている。

【００５０】再生部３２は、制御装置１３から得られたコンテンツ管理情報ＣＭＩに基づいて、再生処理を行なう機能と、再生時には、制御装置１３から読み出した暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を復号してコンテンツ暗号化鍵Ｋｃを得る機能と、ＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒから暗号化されたコンテンツデータＥ［Ｃ］を読み出す機能と、読み出した暗号化されたコンテンツデータＥ［Ｃ］をコンテンツ暗号化鍵Ｋｃにより復号する機能と、復号により得たコンテンツデータＣ及びコンテンツ暗号化鍵Ｋｃを伝送用暗号化部３１に出力する機能とをもっている。

【００５１】具体的には再生部３２は、メディア固有鍵生成回路３３、認証・鍵交換部３４、暗号化／復号回路１６－２、管理情報処理回路３６、復号鍵生成回路３７、鍵復号部３８、コンテンツ復号部３９を備えている。

【００５２】メディア固有鍵生成回路３３は、ＤＶＤ－ＲＡＭディスク１１のリードイン領域１１ｉから読み出された暗号化鍵情報及び識別情報ＩＤと、自己のデバイス鍵とに基づいて、メディア固有鍵Ｋｍを生成して暗号化鍵生成回路３７及び認証・鍵交換部３４に送出する機能をもっている。

【００５３】認証・鍵交換部３４は、メディア固有鍵生成回路３３から受けたメディア固有鍵Ｋｍを用いて制御

装置１３の認証・鍵交換部１５との間で認証及び鍵交換処理を行なう機能と、制御装置１３との間で共有鍵Ｋｓを共有する機能とをもっている。

【００５４】暗号化／復号回路１６－２は、制御装置１３から受けた暗号化データを、認証・鍵交換部３４により共有された共有鍵Ｋｓを用いて復号し、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を鍵復号部３８に送出する一方、得られたコンテンツ管理情報ＣＭＩを管理情報処理回路３６に送出する機能をもっている。

【００５５】管理情報処理回路３６は、暗号化／復号回路１６－２から受けたコンテンツ管理情報ＣＭＩを確認して、再生禁止か否かを判定する機能と、判定結果が再生禁止を示すときには再生処理をせずに終了する機能とをもっている。

【００５６】また、管理情報処理回路３６は、判定結果が再生可能を示す場合、再生時には、コンテンツ管理情報ＣＭＩからコンテンツ部分管理情報ｐＣＭＩを抽出する機能と、このコンテンツ部分管理情報ｐＣＭＩを復号鍵生成回路３７に送出すると共に、コンテンツ管理情報ＣＭＩを伝送用暗号器３１に送出する機能と、コンテンツ管理情報ＣＭＩに再生可能回数又はコピー可能回数の減少等の所定の処理を施した後、コンテンツ管理情報ＣＭＩを暗号化／復号回路１６－２に返送する機能とをもっている。

【００５７】復号鍵生成回路３７は、管理情報処理回路３６から受けたコンテンツ部分管理情報ｐＣＭＩと、メディア固有鍵生成回路３３から受けたメディア固有鍵Ｋｍを用いて鍵復号鍵Ｋｋを生成する機能をもっている。

【００５８】鍵復号部３８は、暗号化／復号回路１６－２で復号された暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を、復号鍵生成回路３７により生成された鍵復号鍵Ｋｋに基づいて、復号する機能をもっている。

【００５９】コンテンツ復号部３９は、ＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒから読み出した暗号化されたコンテンツデータＥ［Ｃ］を、鍵復号部３８により復号された暗号化されたコンテンツ鍵Ｋｃに基づいて復号する機能と、復号して得たコンテンツデータＣを伝送用暗号化器３１に出力する機能をもっている。

【００６０】次に、以上のように構成された情報記録媒体、記録装置及び再生装置による情報の記録方法及び再生方法について図５及び図６のフローチャートを用いて説明する。なお、コンテンツデータＣとしては、著作権付きのものを想定しており、この想定は以下の各実施形態でも同様である。

【００６１】（記録方法）伝送用復号器２１は、図３に示すように、記録装置２０内部から受ける夫々暗号化されたコンテンツデータＥ［Ｃ］、コンテンツ暗号化鍵Ｅ［Ｋｃ］及びコンテンツ管理情報Ｅ［ＣＭＩ］を復号し、夫々得られたコンテンツデータＣ、コンテンツ暗号化鍵Ｋｃ及びコンテンツ管理情報ＣＭＩを記録部２２に入力する。

【００６２】記録部２２においては、図３及び図５に示すように、ＤＶＤ－ＲＡＭディスク１１のリードイン領域１１ｉから暗号化鍵情報と識別番号ＩＤを読出すと（ＳＴ１）、メディア固有鍵生成回路２３が、これら暗号化鍵情報及び識別情報ＩＤと自己のデバイス鍵とに基づいてメディア固有鍵Ｋｍを生成し、このメディア固有鍵Ｋｍを暗号化鍵生成回路２５及び認証・鍵交換部２８に送出する。

【００６３】一方、記録部２２の管理情報処理回路２４は、伝送用復号器２１から入力されたコンテンツ管理情報ＣＭＩを確認して（ＳＴ２）、記録禁止か否かを判定し（ＳＴ３）、コンテンツ管理情報ＣＭＩが記録禁止を示すときには以下の記録処理をせずに終了する。では次に、コンテンツ管理情報ＣＭＩが記録可能を示す場合の動作を述べる。

【００６４】記録可能の場合、管理情報処理回路２４は、コンテンツ管理情報ＣＭＩからコンテンツ部分管理情報ｐＣＭＩを抽出し、このコンテンツ部分管理情報ｐＣＭＩを暗号化鍵生成回路２６に送出すると共に、コンテンツ管理情報ＣＭＩを暗号化／復号回路１６－２に送出する。

【００６５】また一方、コンテンツ暗号化部２５は、伝送用復号器２１からのコンテンツ暗号化鍵Ｋｃに基づいて、伝送用復号器２１から入力されたコンテンツデータＣを暗号化し、得られた暗号化されたコンテンツデータＥ［Ｃ］をＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む（ＳＴ４）。

【００６６】しかる後、暗号化鍵生成回路２６は、コンテンツ部分管理情報ｐＣＭＩ及びメディア固有鍵Ｋｍに基づいて鍵暗号化鍵Ｋｋを生成し、この鍵暗号化鍵Ｋｋを鍵暗号化部２７に送出する。

【００６７】鍵暗号化部２７は、この鍵暗号化鍵Ｋｋを用いてコンテンツ暗号化鍵Ｋｃを暗号化し（ＳＴ５）、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を暗号化／復号回路１６－２に送出する。

【００６８】次に、認証・鍵交換部２８は、メディア固有鍵Ｋｍを用いて制御装置１３の認証・鍵交換部１５との間で認証及び鍵交換（ＡＫＥ）処理を行ない（ＳＴ６）、制御装置１３との間で共有鍵Ｋｓを共有する。

【００６９】暗号化／復号回路１６－２は、この共有鍵Ｋｓに基づいて、暗号化されたコンテンツ鍵Ｅ［Ｋｃ］及びコンテンツ管理情報ＣＭＩを暗号化し、得られた暗号化データを制御装置１３に送る（ＳＴ７）。

【００７０】制御装置１３は、暗号化／復号回路１６－１が、共有鍵Ｋｓに基づいて、この暗号化データを復号し、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］とコンテンツ管理情報ＣＭＩをメモリ１７に記録する（ＳＴ８）。

【００７１】（再生方法）再生部３２においては、図４

及び図６に示すように、ＤＶＤ－ＲＡＭディスク１１のリードイン領域１１ｉから暗号化鍵情報と識別番号ＩＤを読出すと（ＳＴ１１）、メディア固有鍵生成回路３３が、これら暗号化鍵情報及び識別情報ＩＤと、自己のデバイス鍵とに基づいて、メディア固有鍵Ｋｍを生成して暗号化鍵生成回路３７及び認証・鍵交換部３４に送出する。

【００７２】次に、認証・鍵交換部３４は、メディア固有鍵Ｋｍを用いて制御装置１３の認証・鍵交換部１５との間で認証及び鍵交換処理を行ない（ＳＴ１２）、制御装置１３との間で共有鍵Ｋｓを共有する。

【００７３】制御装置１３では、暗号化／復号回路１６－１が、メモリ１７から読み出した暗号化されたコンテンツ鍵Ｅ［Ｋｃ］とコンテンツ管理情報ＣＭＩを共有鍵Ｋｓにより暗号化し、得られた暗号化データを再生部３２に送る（ＳＴ１３）。

【００７４】再生部３２では、暗号化／復号回路１６－２が、この暗号化データを共有鍵Ｋｓにより復号し、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を鍵復号部３８に送出する一方、得られたコンテンツ管理情報ＣＭＩを管理情報処理回路３６に送出する（ＳＴ１４）。

【００７５】管理情報処理回路３６は、このコンテンツ管理情報ＣＭＩを確認し（ＳＴ１５）、再生禁止か否かを判定し（ＳＴ１６）、コンテンツ管理情報ＣＭＩが再生禁止を示すときには以下の再生処理をせずに終了する。では次に、コンテンツ管理情報ＣＭＩが再生可能を示す場合の動作を述べる。

【００７６】再生可能の場合、管理情報処理回路３６は、コンテンツ管理情報ＣＭＩからコンテンツ部分管理情報ｐＣＭＩを抽出し、このコンテンツ部分管理情報ｐＣＭＩを復号鍵生成回路３７に送出すると共に、コンテンツ管理情報ＣＭＩを伝送用暗号器３１に送出する。

【００７７】さらに、管理情報処理回路３６は、コンテンツ管理情報ＣＭＩに再生可能回数又はコピー可能回数の減少等の所定の更新処理を施した後（ＳＴ１７）、コンテンツ管理情報ＣＭＩを暗号化／復号回路１６－２により暗号化して制御装置１３に送出する。制御装置１３は、暗号化されたコンテンツ管理情報ＣＭＩを復号してメモリ１７に記録する。

【００７８】次に、再生部３２では、復号鍵生成回路３７が、コンテンツ部分管理情報ｐＣＭＩとステップＳＴ１１で求めたメディア固有鍵Ｋｍを用いて鍵復号鍵Ｋｋを生成し、この鍵復号鍵Ｋｋを鍵復号部３８に送出する。

【００７９】鍵復号部３８は、この鍵復号鍵Ｋｋに基づいて、暗号化／復号回路１６－２で得た暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を復号し、得られたコンテンツ暗号化鍵Ｋｃをコンテンツ復号部３９に送出する（ＳＴ１８）。なお、これに加え、必要によりコンテンツ暗号化鍵Ｋｃを伝送用暗号化器３１に出力してもよい。

【００８０】しかる後、再生部３２では、コンテンツ復号部３９が、ＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒから暗号化されたコンテンツデータＥ［Ｃ］を読み出し、この暗号化されたコンテンツデータＥ［Ｃ］をコンテンツ暗号化鍵Ｋｃにより復号し、得られたコンテンツデータＣを伝送用暗号化器３１に出力する（ＳＴ１９）。

【００８１】伝送用暗号化器３１は、このコンテンツデータを再生装置の方式に対応した任意の方式で暗号化し、得られた暗号化されたコンテンツデータＥ’［Ｃ］を出力する。

【００８２】上述したように本実施形態によれば、認証機能により認証され、且つ管理情報により記録／再生可能とされたときのみ、コンテンツデータＣを記録／再生できる情報記録媒体１０、記録装置２０及び再生装置３０が実現されるため、コンテンツデータを記録可能で、且つ不正な利用から保護することができる。

【００８３】すなわち、ＤＶＤ－ＲＡＭディスク１１等の如き、情報記録機能のみをもつ単純な記録媒体においても、ＤＶＤ－ＲＡＭディスク１１から離して制御装置１３を設けるという簡単な拡張により、複雑なセキュリティ機能を実現させることができる。

【００８４】例えば、ＤＶＤ－ＲＡＭディスク１１の内容をコピーしたとしても、制御装置１３のメモリ１７内容やメディア固有鍵Ｋｐをコピーできないため、ディスク１１のコピーを利用することができず、結果として不正なコピーの頒布を阻止している。

【００８５】また、周知のＤＶＤ－ＲＡＭプレーヤ／レコーダおよびＤＶＤ－ＲＡＭドライブ等の記録装置２０及び再生装置３０の形状を一切変更せずに、その内部に、制御装置１３の認証、データの暗号化／復号、管理情報の確認といったセキュリティ動作をする回路（記録部２２や再生部３２等）を追加するだけで、高度なセキュリティ機能を実現することができる。

【００８６】また、制御装置１３としては、ＤＶＤ－ＲＡＭディスク１１から読み出された識別番号ＩＤ等から記録装置２０又は再生装置３０が作成したメディア固有鍵Ｋｍに基づいて、認証処理を実行する構成であり、すなわち、ＤＶＤ－ＲＡＭディスク１１と制御装置１３との組合せが一致しないと記録／再生装置２０，３０を認証しないので、制御装置１３又はＤＶＤ－ＲＡＭディスク１１の付替えといった改造による不正をも阻止することができる。

【００８７】また、制御装置１３が保護ケース１２に取り付けられた簡易な構成で実現できるので、本発明の情報記録媒体１０を容易且つ確実に製造することができる。

【００８８】また、ＤＶＤ－ＲＡＭディスク１１と制御装置１３とは、互いに離間して設けられるので、固定的に設けられた制御装置１３と、回転可能な媒体部（例、

ディスク、テープ等）という構成により容易に実現できる。

【００８９】（第２の実施形態）図７は本発明の第２の実施形態に係る記録装置及び情報記録媒体の構成を示す模式図であり、図８は同実施形態における再生装置及び情報記録媒体の構成を示す模式図であって、図３及び図４と同一部分には同一符号を付し、異なる部分にはａの添字を付して説明し、ここでは異なる部分について主に述べる。

【００９０】すなわち、本実施形態が第１の実施形態と異なる点は、主に、（１）コンテンツ部分管理情報ｐＣＭＩを利用せず、コンテンツ管理情報ＣＭＩ内に設けたコピー管理情報ＣＣＩを鍵暗号化鍵Ｋｋ及び鍵復号鍵Ｋｋの生成に用いる点と、（２）このコピー管理情報ＣＣＩをＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに記録する点と、（３）暗号化されたコンテンツ鍵Ｅ［Ｋｃ］の記録場所を制御装置１３ではなく、ＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒとした点と、である。

【００９１】これらの変更点に伴い、記録装置２０ａは、変更された機能ブロックとして、管理情報処理回路２４ａ、暗号鍵生成回路２６ａ及び鍵暗号化部２７ａを備えている。

【００９２】管理情報処理回路２４ａは、伝送用復号器２１から受けたコンテンツ管理情報ＣＭＩ内のコピー管理情報ＣＣＩに基づいて記録禁止か否かを判定する機能と、コピー管理情報ＣＣＩが記録禁止を示すときには記録処理をせずに終了する機能とをもっている。

【００９３】また、管理情報処理回路２４ａは、コピー管理情報ＣＣＩが記録可能を示す場合、コピー管理情報ＣＣＩをＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む一方、暗号化鍵生成回路２６ａに送出する機能をもっている。

【００９４】ここで、コピー管理情報ＣＣＩは、コンテンツ管理情報ＣＭＩのうち、コピー管理に関する部分である。コピー管理情報ＣＣＩには、自由にコピー可能な“Copy Freely”、１回だけコピー可能な“Copy One Generation”、それ以上のコピーが禁止される“No More Copies”及び絶対にコピー禁止の“Never Copy”の４つの状態が存在するが、コピー可能であり暗号化等によって、記録媒体上でコンテンツを守る必要がある状態は、“Copy One Generation”のみである。さらに“Copy One Generation”のコンテンツは、１回コピーした後、“No More Copies”の状態で記録される（コピー毎に可能回数が１回減る）。従って、殆どの場合、ここで鍵生成に使われるコピー管理情報はＣＣＩ＝“No More Copies”である。

【００９５】暗号化鍵生成回路２６ａは、管理情報処理回路２４ａから受けたコピー管理情報ＣＣＩと、前述同様にメディア固有鍵生成回路２３から受けたメディア固有鍵Ｋｍとに基づいて、鍵暗号化鍵Ｋｋを生成する機能と、この鍵暗号化鍵Ｋｋを鍵暗号化部２７ａに送出する機能とをもっている。

【００９６】鍵暗号化部２７ａは、暗号鍵生成回路２６ａから受けた鍵暗号化鍵Ｋｋを用いてコンテンツ暗号化鍵Ｋｃを暗号化する前述した機能に加え、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を（暗号化／復号回路１６－２経由ではなく）ＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む機能とをもっている。

【００９７】一方、再生装置３０ａは、変更された機能ブロックとして、管理情報処理回路３６ａ、復号鍵生成回路３７ａ及び鍵復号部３８ａを備えている。

【００９８】管理情報処理回路３６ａは、暗号化／復号回路１６－２から受けたコンテンツ管理情報ＣＭＩを確認する機能と、コンテンツ管理情報ＣＭＩに再生可能回数又はコピー可能回数の減少等の所定の更新処理を施した後、伝送用暗号化器３１に出力する機能と、当該コンテンツ管理情報ＣＭＩを暗号化／復号回路１６－２により暗号化して制御装置１３に送出する機能とをもっている。

【００９９】復号鍵生成回路３７ａは、ＤＶＤ－ＲＡＭディスク１１から読み出されたコピー管理情報ＣＣＩと、前述同様にメディア固有鍵生成回路２３から受けたメディア固有鍵Ｋｍとに基づいて鍵復号鍵Ｋｋを生成する機能と、得られた鍵復号鍵Ｋｋを鍵復号部３８ａに送出する機能とをもっている。

【０１００】鍵復号部３８ａは、ＤＶＤ－ＲＡＭディスク１１から読み出された暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を、復号鍵生成回路３７ａから受けた鍵復号鍵Ｋｋに基づいて復号する機能と、得られたコンテンツ暗号化鍵Ｋｃをコンテンツ復号部３９に送出する機能とをもっている。

【０１０１】次に、以上のように構成された情報記録媒体、記録装置及び再生装置による情報の記録方法及び再生方法について図９及び図１０のフローチャートを用いて説明する。

【０１０２】（記録方法）図７及び図９に示すように、記録部２２ａにおいては、前述同様に、ステップＳＴ１のＩＤ等の読出からメディア固有鍵Ｋｍの生成並びにステップＳＴ２のコンテンツ管理情報ＣＭＩの確認までを行なう。次に、記録部２２ａの管理情報処理回路２４ａは、コンテンツ管理情報ＣＭＩ内のコピー管理情報ＣＣＩに基づいて記録禁止か否かを判定し（ＳＴ３ａ）、コピー管理情報ＣＣＩが記録禁止を示すときには以下の記録処理をせずに終了する。では次に、コピー管理情報ＣＣＩが記録可能を示す場合の動作を述べる。

【０１０３】記録可能な場合、コンテンツ暗号化部２５は、前述同様に、ステップＳＴ４を行ない、暗号化されたコンテンツデータＥ［Ｃ］をＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む。

【０１０４】また、管理情報処理回路２４ａは、コピー

管理情報ＣＣＩをＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む一方（ＳＴ４－２）、暗号化鍵生成回路２６に送出する。

【０１０５】暗号化鍵生成回路２６ａは、このコピー管理情報ＣＣＩとステップＳＴ１で得たメディア固有鍵Ｋｍとに基づいて鍵暗号化鍵Ｋｋを生成し、この鍵暗号化鍵Ｋｋを鍵暗号化部２７ａに送出する。

【０１０６】鍵暗号化部２７ａは、この鍵暗号化鍵Ｋｋを用いてコンテンツ暗号化鍵Ｋｃを暗号化し（ＳＴ５）、得られた暗号化されたコンテンツ鍵Ｅ［Ｋｃ］をＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに書込む（ＳＴ５－２）。

【０１０７】以下前述同様に、記録部２２ａは、ステップＳＴ６の認証及び鍵交換処理を行ない、制御装置１３との間で共有鍵Ｋｓを共有する。

【０１０８】また、暗号化／復号回路１６－２は、この共有鍵Ｋｓに基づいて、コンテンツ管理情報ＣＭＩを暗号化し、得られた暗号化データを制御装置１３に送る（ＳＴ７ａ）。

【０１０９】制御装置１３では、暗号化／復号回路１６－１が、共有鍵Ｋｓに基づいて、この暗号化データを復号し、得られたコンテンツ管理情報ＣＭＩをメモリ１７に記録する（ＳＴ８ａ）。

【０１１０】（再生方法）図８及び図１０に示すように、再生部３２ａにおいては、前述同様に、ステップＳＴ１１のＩＤ等の読出により、メディア固有鍵Ｋｍの生成を行なう。

【０１１１】次に、再生部３２ａは、ＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒから暗号化されたコンテンツ鍵Ｅ［Ｋｃ］とコピー管理情報ＣＣＩとを読み出し（ＳＴ２１）、復号鍵生成回路３７ａが、このコピー管理情報ＣＣＩとメディア固有鍵Ｋｍを用いて鍵復号鍵Ｋｋを生成し、得られた鍵復号鍵Ｋｋを鍵復号部３８ａに送出する。

【０１１２】鍵復号部３８ａは、この鍵復号鍵Ｋｋに基づいて、暗号化されたコンテンツ鍵Ｅ［Ｋｃ］を復号し、得られたコンテンツ暗号化鍵Ｋｃをコンテンツ復号部３９に送出する（ＳＴ２２）。

【０１１３】コンテンツ復号部３９は、ＤＶＤ－ＲＡＭディスク１１から暗号化されたコンテンツデータＥ［Ｃ］を読み出し（ＳＴ２３）、コンテンツ暗号化鍵Ｋｃを用いて暗号化されたコンテンツデータＥ［Ｃ］を復号し、得られたコンテンツデータＣを出力する（ＳＴ２４）。この時、必要に応じてコンテンツ暗号化鍵Ｋｃもコンテンツ復号部３９又は鍵復号部３８ａから出力される。

【０１１４】再生部３２ａでは、ステップＳＴ１２と同様に認証及び鍵交換（ＡＫＥ）処理を行ない（ＳＴ１２）、制御装置１３の間で共有鍵Ｋｓを共有する。

【０１１５】制御装置１３は、暗号化／復号回路１６－１が、メモリ１７から読み出したコンテンツ管理情報ＣＭＩを共有鍵Ｋｓにより暗号化し、得られた暗号化データを再生部３２ａに送る（ＳＴ１３ａ）。

【０１１６】再生部３２ａでは、暗号化／復号回路１６－２が、この暗号化データを共有鍵Ｋｓにより復号し、得られたコンテンツ管理情報ＣＭＩを管理情報処理回路３６ａに送出する（ＳＴ１４ａ）。

【０１１７】管理情報処理回路３６ａは、コンテンツ管理情報ＣＭＩを確認し（ＳＴ１５ａ）、コンテンツ管理情報ＣＭＩに再生可能回数又はコピー可能回数の減少等の所定の更新処理を施す（ＳＴ１７ａ）。ここでは特に、ステップＳＴ１５ａの確認の際に、コンテンツ管理情報ＣＭＩが再生禁止を示したとき、コピー管理情報ＣＣＩを変更する（これにより、次回の再生時に、復号鍵生成回路３７ａが鍵復号鍵Ｋｋを正しく生成できないようにし、もって、コンテンツデータＣを正しく復号できなくする）。

【０１１８】しかる後、管理情報処理回路３６ａは、コンテンツ管理情報ＣＭＩを伝送用暗号化器３１に出力する一方、当該コンテンツ管理情報ＣＭＩを暗号化／復号回路１６－２により暗号化して制御装置１３に送出する（ＳＴ２５）。制御装置１３は、暗号化されたコンテンツ管理情報ＣＭＩを復号してメモリ１７に記録する（ＳＴ２６）。

【０１１９】上述したように本実施形態によれば、

（１）コンテンツ管理情報ＣＭＩ内に設けたコピー管理情報ＣＣＩを鍵暗号化鍵Ｋｋ及び鍵復号鍵Ｋｋの生成に用い、（２）このコピー管理情報ＣＣＩをＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒに記録し、（３）暗号化されたコンテンツ鍵Ｅ［Ｋｃ］の記録場所をＤＶＤ－ＲＡＭディスク１１の記録領域１１ｒとした構成に変形しても、第１の実施形態と同様の効果を得ることができる。

【０１２０】なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０１２１】また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１２２】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【０１２３】さらに、本発明における記憶媒体は、コン

ピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１２４】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１２５】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１２６】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１２７】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。

【０１２８】例えば、媒体部は、ＤＶＤ－ＲＡＭディスク１１に限らず、任意の記録媒体を使用してもよい。また、記録方法や再生方法は、細かい手順を適宜、前後させてもよい。

【０１２９】例えば、第１の実施形態の記録方法において、コンテンツ管理情報ＣＭＩに基づく記録禁止か否かの判定（ＳＴ３）を、暗号化鍵情報及び識別情報ＩＤの読出（ＳＴ１）よりも先に行なっても良く、また、暗号化されたコンテンツデータＥ［Ｃ］の書込（ＳＴ４）を、暗号化されたコンテンツ鍵Ｅ［Ｋｃ］及びコンテンツ管理情報ＣＭＩの記録（ＳＴ８）よりも後に行なっても良い。また、認証及び鍵交換（ＳＴ６）を、暗号化されたコンテンツデータＥ［Ｃ］の書込（ＳＴ４）よりも先に行ない、認証及び鍵交換（ＳＴ６）の結果が良いときのみ、ＳＴ４を許可する手順としてもよい。

【０１３０】いずれにしても、記録禁止か否かの判定（ＳＴ３）の後に、暗号化されたコンテンツデータＥ［Ｃ］の書込（ＳＴ４）が行われる手順であれば、図３の矢印が上流から下流に向かう範囲で他の手順を適宜、前後させてもよい。

【０１３１】同様に、第１の実施形態の再生方法において、例えば、コンテンツ管理情報ＣＭＩの更新（ＳＴ１７）を、コンテンツデータＣの出力（ＳＴ１９）よりも後に行なっても良い。

【０１３２】すなわち、再生禁止か否かの判定（ＳＴ１６）の後に、コンテンツデータＣの出力（ＳＴ１９）が行われる手順であれば、図４の矢印が上流から下流に向かう範囲で他の手順を適宜、前後させてもよい。

【０１３３】これらの変形可能な例は第２の実施形態でも同様である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【０１３４】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【０１３５】

【発明の効果】以上説明したように本発明によれば、コンテンツデータを記録可能で、且つ不正な利用から保護することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る情報記録媒体の構成を示す模式図

【図２】同実施形態における情報記録媒体の構成を示す模式図

【図３】同実施形態における情報記録媒体及び記録装置の構成を示す模式図

【図４】同実施形態における情報記録媒体及び再生装置の構成を示す模式図

【図５】同実施形態における記録方法を説明するためのフローチャート

【図６】同実施形態における再生方法を説明するためのフローチャート

【図７】本発明の第２の実施形態に係る記録装置及び情報記録媒体の構成を示す模式図

【図８】同実施形態における再生装置及び情報記録媒体の構成を示す模式図

【図９】同実施形態における記録方法を説明するためのフローチャート

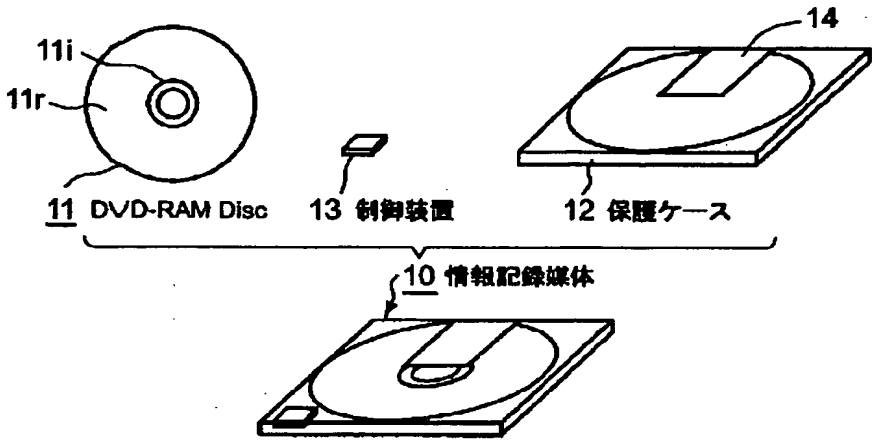
【図１０】同実施形態における再生方法を説明するためのフローチャート

【符号の説明】

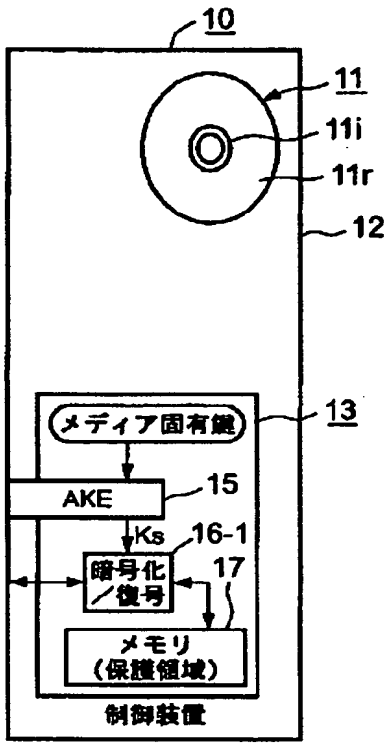
１１…ＤＶＤ－ＲＡＭディスク
１１ｉ…リードイン領域
１１ｒ…記録領域
１２…保護ケース
１３…制御装置
１４…スライド蓋付窓部
１５，２８，３４…認証・鍵交換部
１６－１，１６－２…暗号化／復号回路
１７…メモリ
２０…記録装置
２１…伝送用復号器
２２…記録部
２３，３３…メディア固有鍵生成回路
２４，２４ａ，３６，３６ａ…管理情報処理回路
２５…コンテンツ暗号化部

２６，２６ａ…暗号化鍵生成回路
２７，２７ａ…鍵暗号化部
３０…再生装置
３１…伝送用暗号化器
３２…再生部
３７，３７ａ…復号鍵生成回路
３８，３８ａ…鍵復号部
３９…コンテンツ復号部

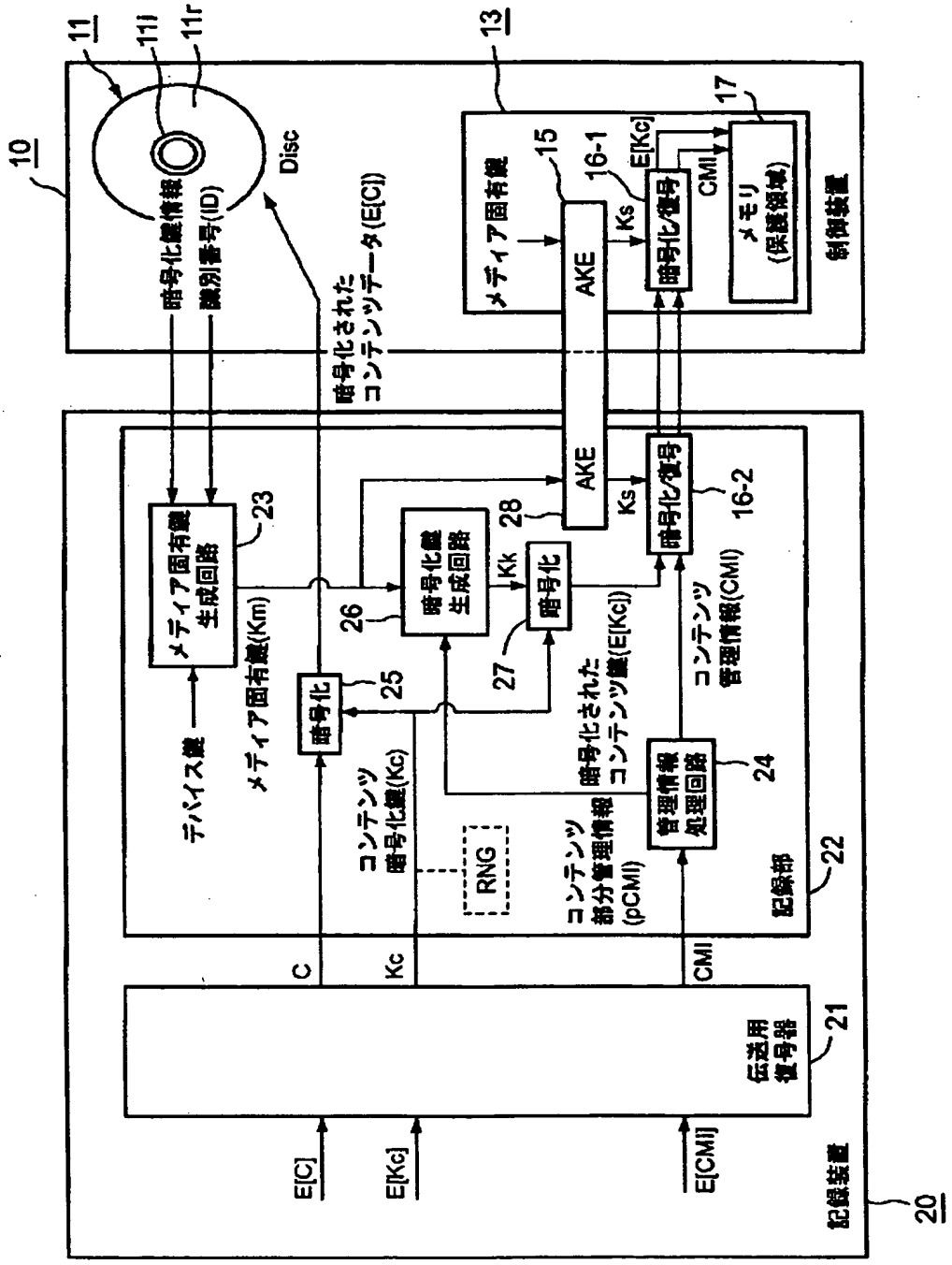
【図１】



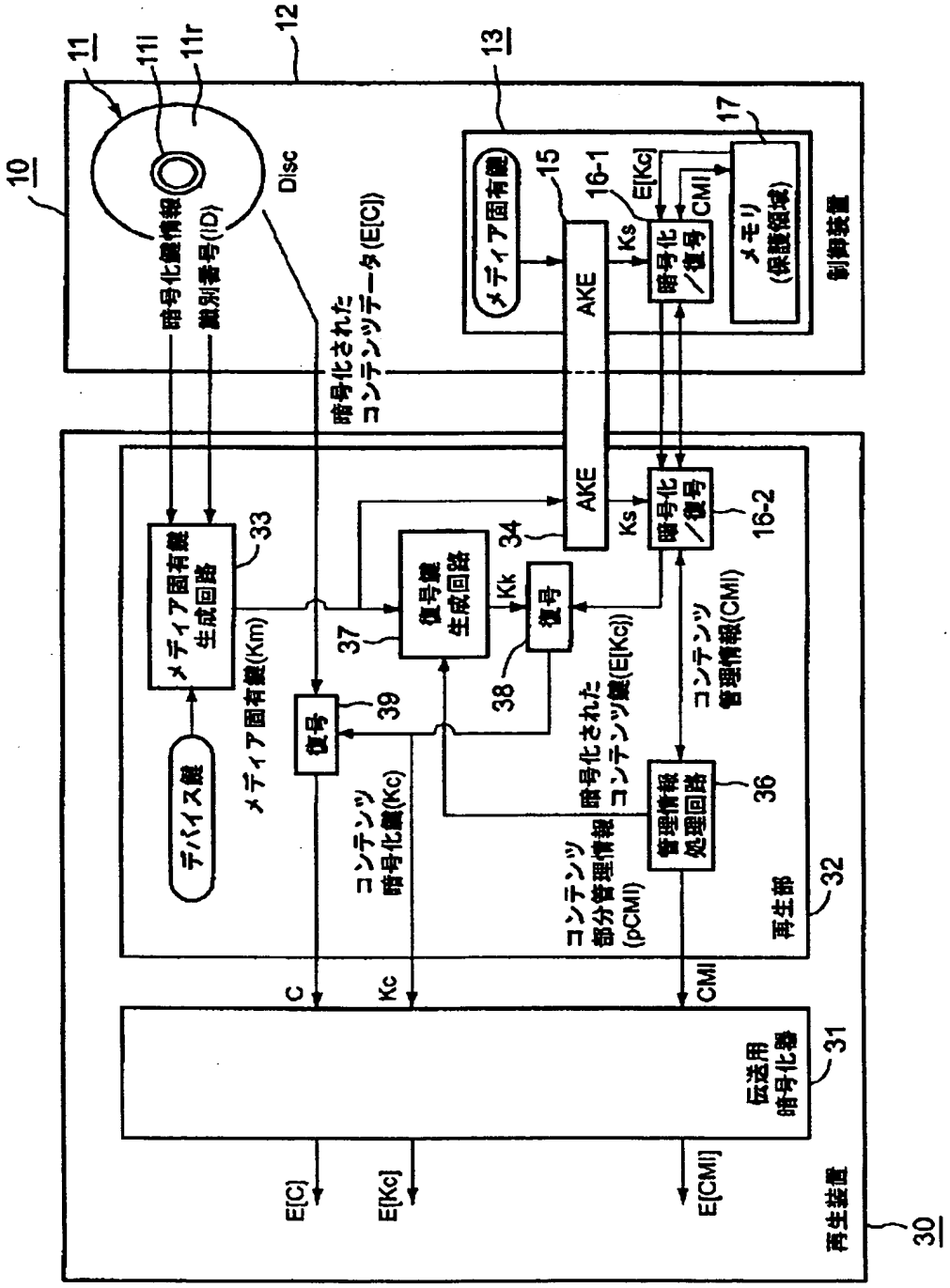
【図２】



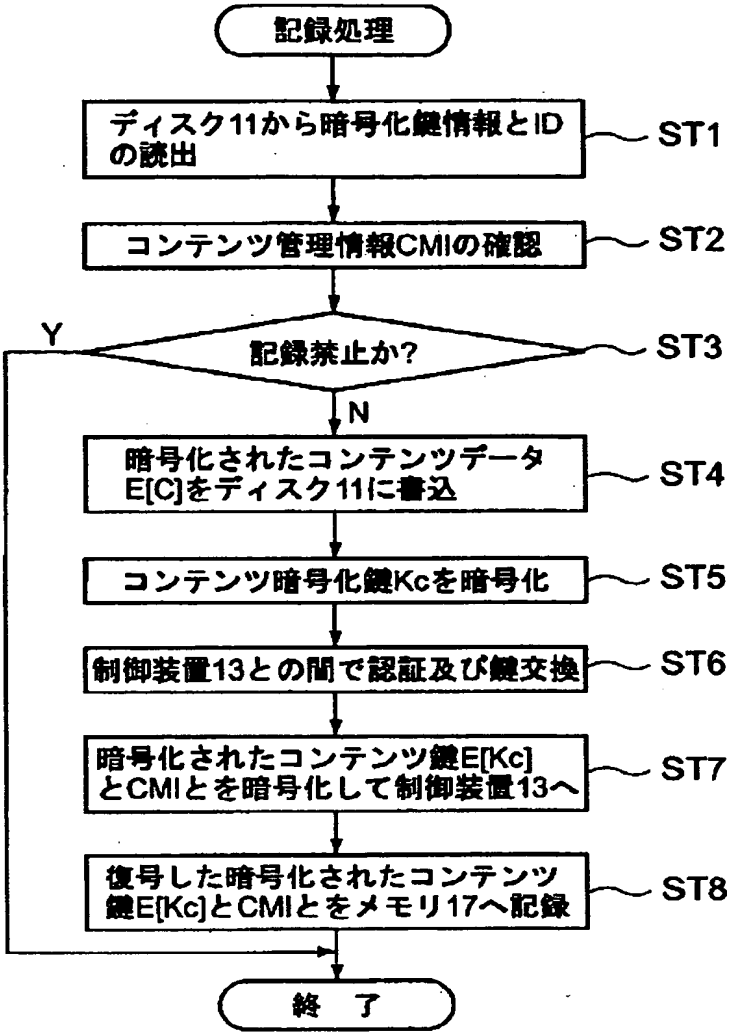
【図３】


10
11
11i
11r
暗号化鍵情報
識別番号(ID)
Disc
暗号化された
コンテンツデータ(E[C])
13
メディア固有鍵
15
AKE
16-1
E[Kc]
CMI
17
暗号化/復号
メモリ
(保護領域)
制御装置
AKE
Ks
暗号化/復号
16-2
メディア固有鍵
生成回路
23
暗号化鍵
生成回路
28
Kk
暗号化
26
27
暗号化
25
デバイス鍵
メディア固有鍵(Km)
コンテンツ
暗号化鍵(Kc)
RNG
暗号化された
コンテンツ鍵(E[Kc])
コンテンツ
管理情報(CMI)
管理情報
処理回路
24
コンテンツ
部分管理情報
(pCMI)
記録部
22
C
Kc
CMI
伝送用
信号部
21
E[C]
E[Kc]
E[CMI]
記録装置
20

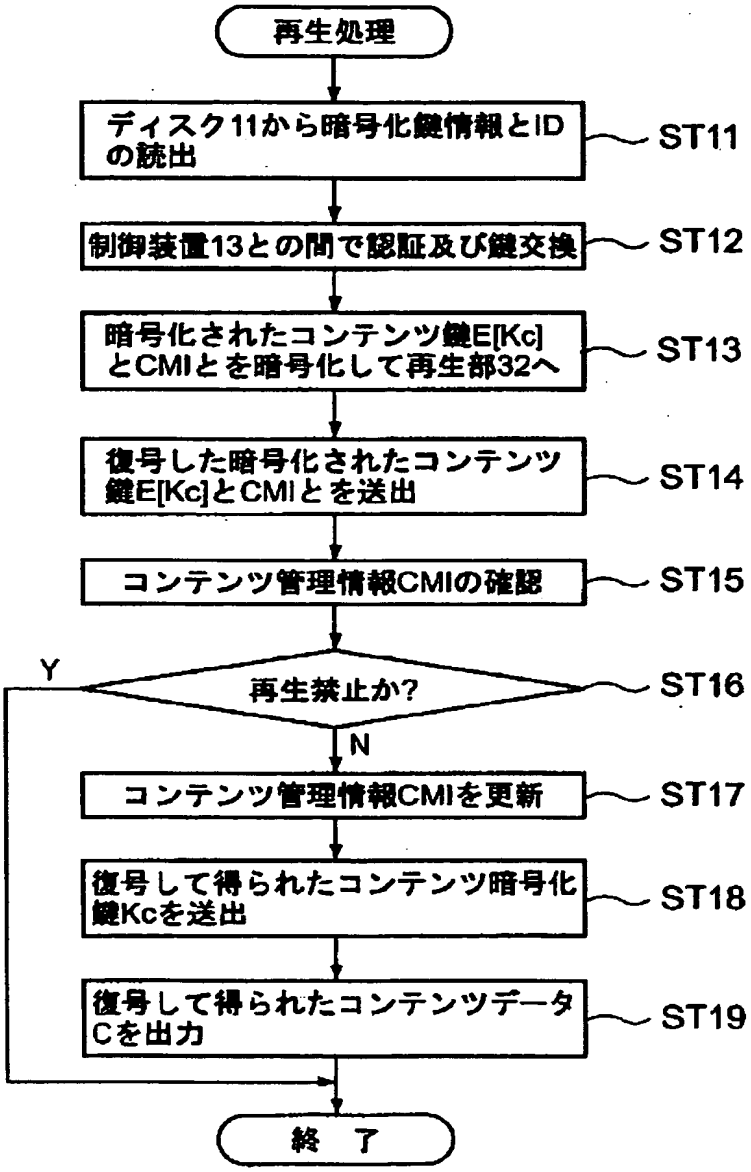
【図４】


10
11
11l
11r
12
13
Disc
暗号化鍵情報
識別番号(ID)
暗号化されたコンテンツデータ(E[C])
メディア固有鍵
AKE
暗号化/復号
メモリ(保護領域)
制御装置
15
16-1
16-2
17
E[Kc]
CMI
Ks
Kk
33
34
37
38
39
メディア固有鍵生成回路
復号鍵生成回路
復号
デバイス鍵
メディア固有鍵(Km)
コンテンツ暗号化鍵(Kc)
暗号化されたコンテンツ鍵(E[Kc])
コンテンツ管理情報(CMI)
コンテンツ部分管理情報(pCMI)
管理情報処理回路
36
32
再生部
C
Kc
CMI
伝送用暗号化器
31
E[C]
E[Kc]
E[CMI]
再生装置
30

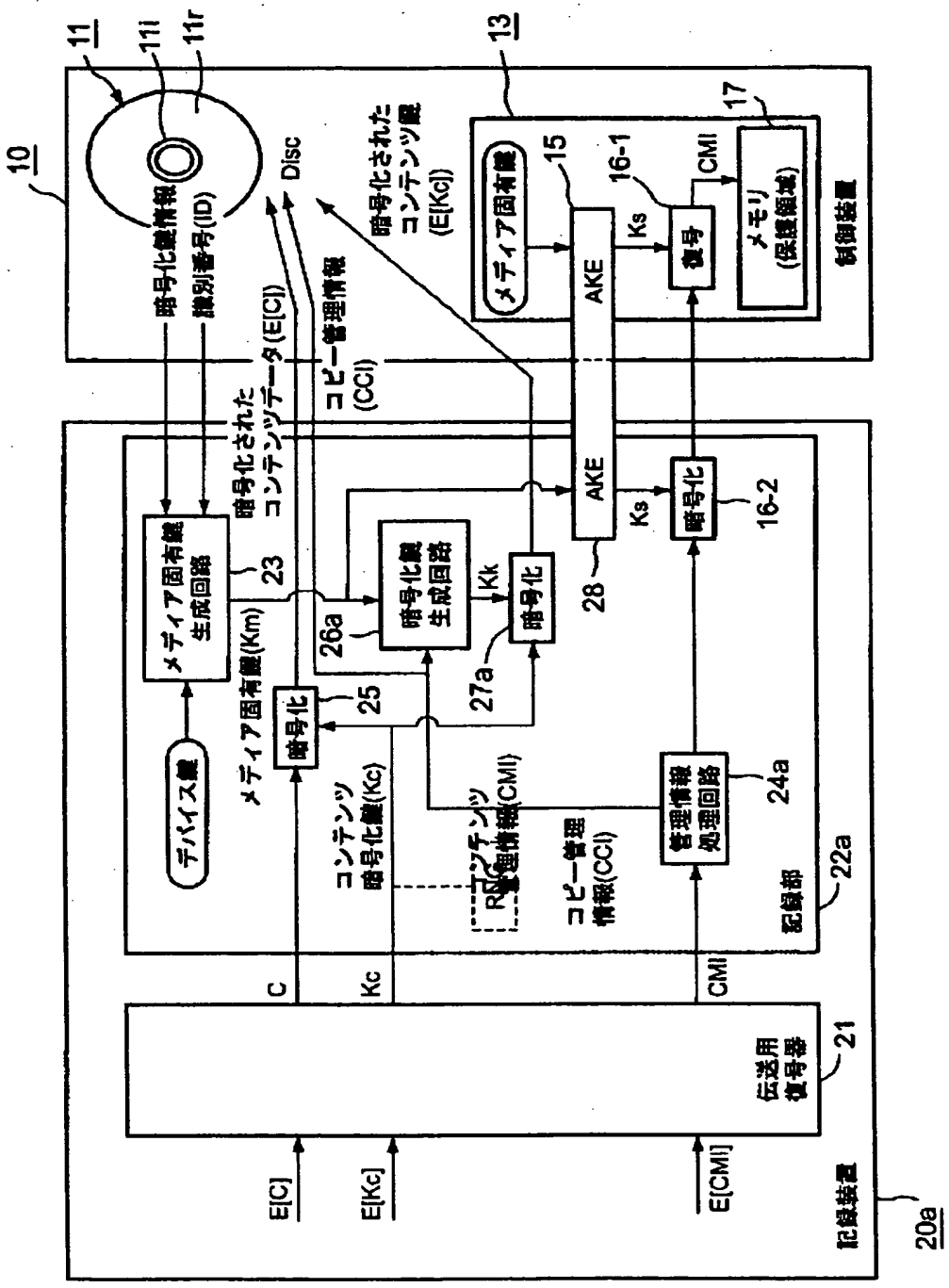
【図５】


記録処理
ディスク11から暗号化鍵情報とIDの読出
ST1
コンテンツ管理情報CMIの確認
ST2
Y
記録禁止か?
ST3
N
暗号化されたコンテンツデータE[C]をディスク11に書込
ST4
コンテンツ暗号化鍵Kcを暗号化
ST5
制御装置13との間で認証及び鍵交換
ST6
暗号化されたコンテンツ鍵E[Kc]とCMIとを暗号化して制御装置13へ
ST7
復号した暗号化されたコンテンツ鍵E[Kc]とCMIとをメモリ17へ記録
ST8
終　了

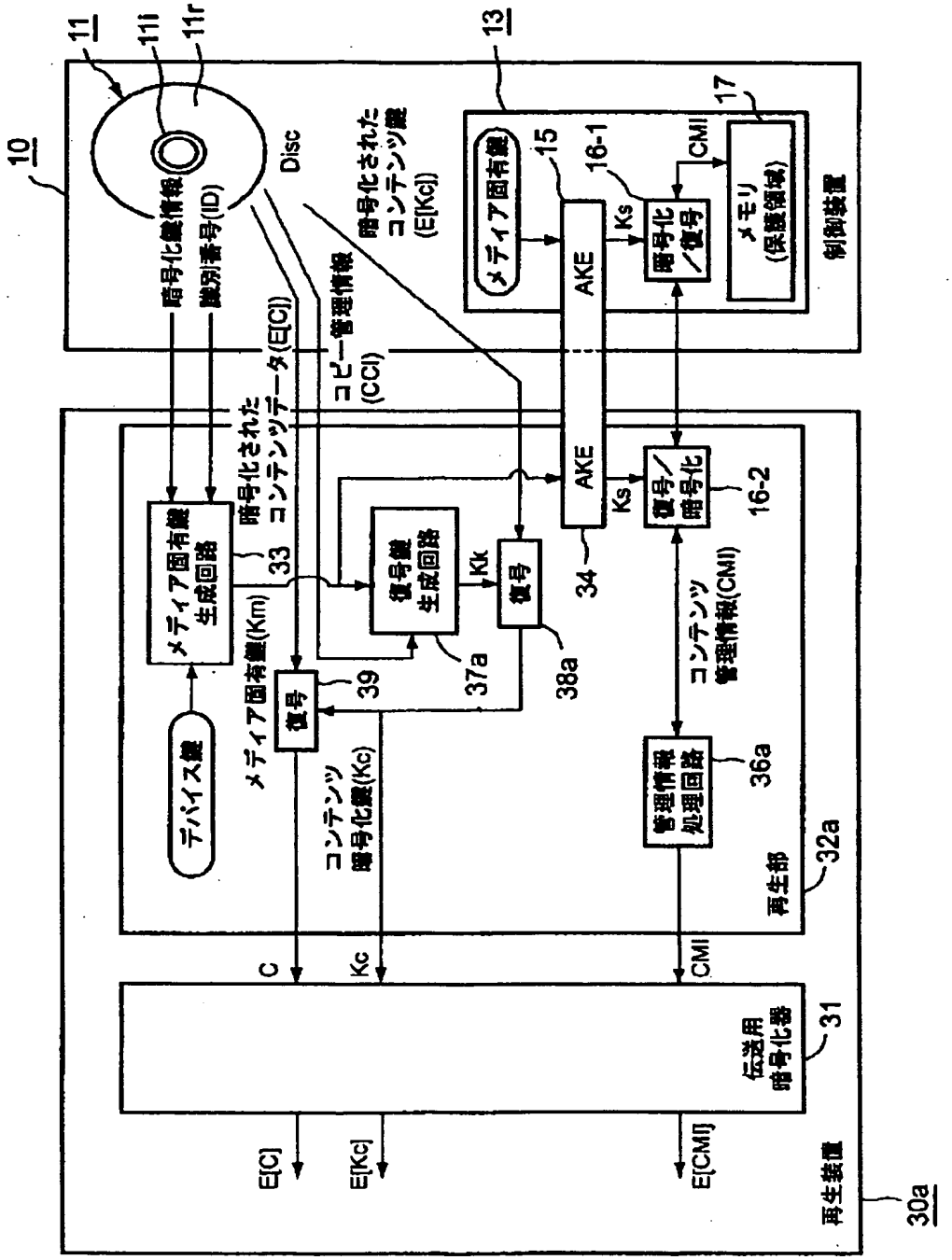
【図６】


再生処理
ディスク11から暗号化鍵情報とIDの読出
ST11
制御装置13との間で認証及び鍵交換
ST12
暗号化されたコンテンツ鍵E[Kc]とCMIとを暗号化して再生部32へ
ST13
復号した暗号化されたコンテンツ鍵E[Kc]とCMIとを送出
ST14
コンテンツ管理情報CMIの確認
ST15
再生禁止か?
ST16
Y
N
コンテンツ管理情報CMIを更新
ST17
復号して得られたコンテンツ暗号化鍵Kcを送出
ST18
復号して得られたコンテンツデータCを出力
ST19
終 了

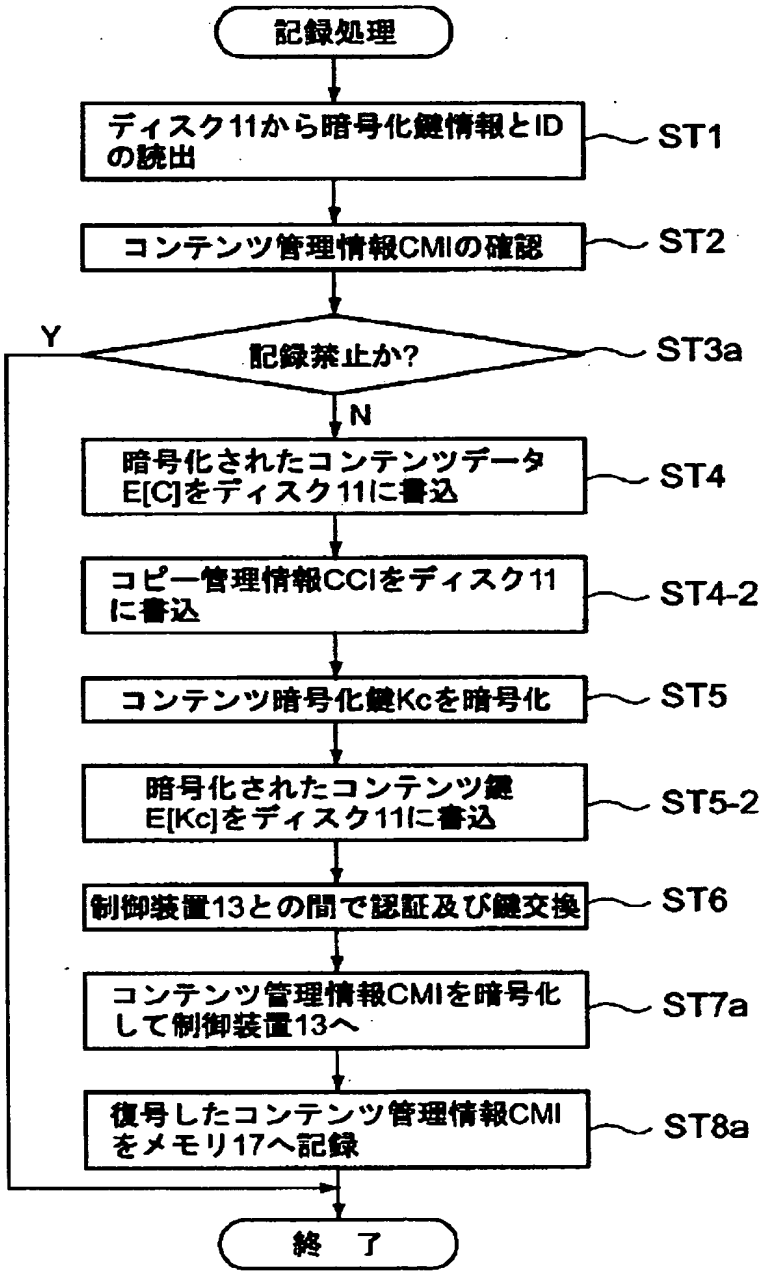
【図７】


11
11i
11r
13
10
Disc
暗号化されたコンテンツ鍵(E[Kc])
17
15
16-1
CMI
メディア固有鍵
AKE
Ks
復号
メモリ(保護領域)
制御装置
暗号化鍵情報
識別番号(ID)
暗号化されたコンテンツデータ(E[C])
コピー管理情報(CCI)
AKE
Ks
暗号化
16-2
メディア固有鍵生成回路
23
暗号化鍵生成回路
Kk
暗号化
28
26a
27a
メディア固有鍵(Km)
暗号化
25
デバイス鍵
コンテンツ暗号化鍵(Kc)
コンテンツ管理情報(CMI)
コピー管理情報(CCI)
管理情報処理回路
24a
記録部
22a
C
Kc
CMI
伝送用復号器
21
E[C]
E[Kc]
E[CMI]
記録装置
20a

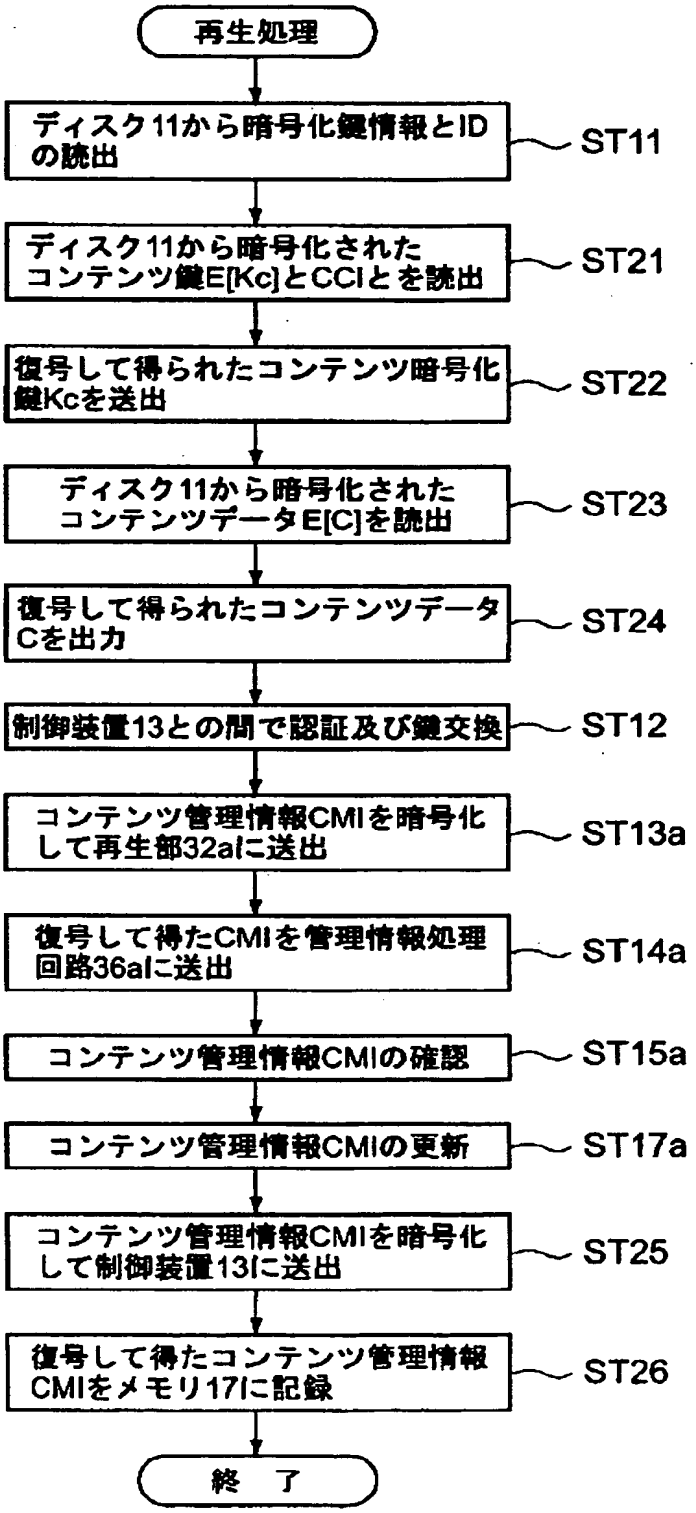
【図８】


10
11
11i
11r
暗号化鍵情報
識別番号(ID)
Disc
暗号化されたコンテンツ鍵(E[Kc])
13
17
CMI
メディア固有鍵
15
16-1
AKE
Ks
暗号化/復号
メモリ(保護領域)
制御装置
コピー管理情報(CCI)
暗号化されたコンテンツデータ(E[C])
AKE
Ks
復号/暗号化
16-2
メディア固有鍵生成回路
33
メディア固有鍵(Km)
復号鍵生成回路
Kk
復号
34
デバイス鍵
復号
39
37a
38a
コンテンツ管理情報(CMI)
コンテンツ暗号化鍵(Kc)
管理情報処理回路
36a
再生部
32a
C
Kc
CMI
伝送用暗号化器
31
E[C]
E[Kc]
E[CMI]
再生装置
30a

【図９】


記録処理
ディスク11から暗号化鍵情報とIDの読出
ST1
コンテンツ管理情報CMIの確認
ST2
Y
記録禁止か?
ST3a
N
暗号化されたコンテンツデータE[C]をディスク11に書込
ST4
コピー管理情報CCIをディスク11に書込
ST4-2
コンテンツ暗号化鍵Kcを暗号化
ST5
暗号化されたコンテンツ鍵E[Kc]をディスク11に書込
ST5-2
制御装置13との間で認証及び鍵交換
ST6
コンテンツ管理情報CMIを暗号化して制御装置13へ
ST7a
復号したコンテンツ管理情報CMIをメモリ17へ記録
ST8a
終 了

【図１０】


再生処理
ディスク11から暗号化鍵情報とIDの読出
ST11
ディスク11から暗号化されたコンテンツ鍵E[Kc]とCCIとを読出
ST21
復号して得られたコンテンツ暗号化鍵Kcを送出
ST22
ディスク11から暗号化されたコンテンツデータE[C]を読出
ST23
復号して得られたコンテンツデータCを出力
ST24
制御装置13との間で認証及び鍵交換
ST12
コンテンツ管理情報CMIを暗号化して再生部32aに送出
ST13a
復号して得たCMIを管理情報処理回路36aに送出
ST14a
コンテンツ管理情報CMIの確認
ST15a
コンテンツ管理情報CMIの更新
ST17a
コンテンツ管理情報CMIを暗号化して制御装置13に送出
ST25
復号して得たコンテンツ管理情報CMIをメモリ17に記録
ST26
終　了

フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	テーマコード(参考)
H04N 5/92		H04N 5/92	H